TWG-98-77

Proposed Directory Implementation for the Federal Public Key Infrastructure

Briefing for the Federal Public Key Infrastructure Technical Working Group

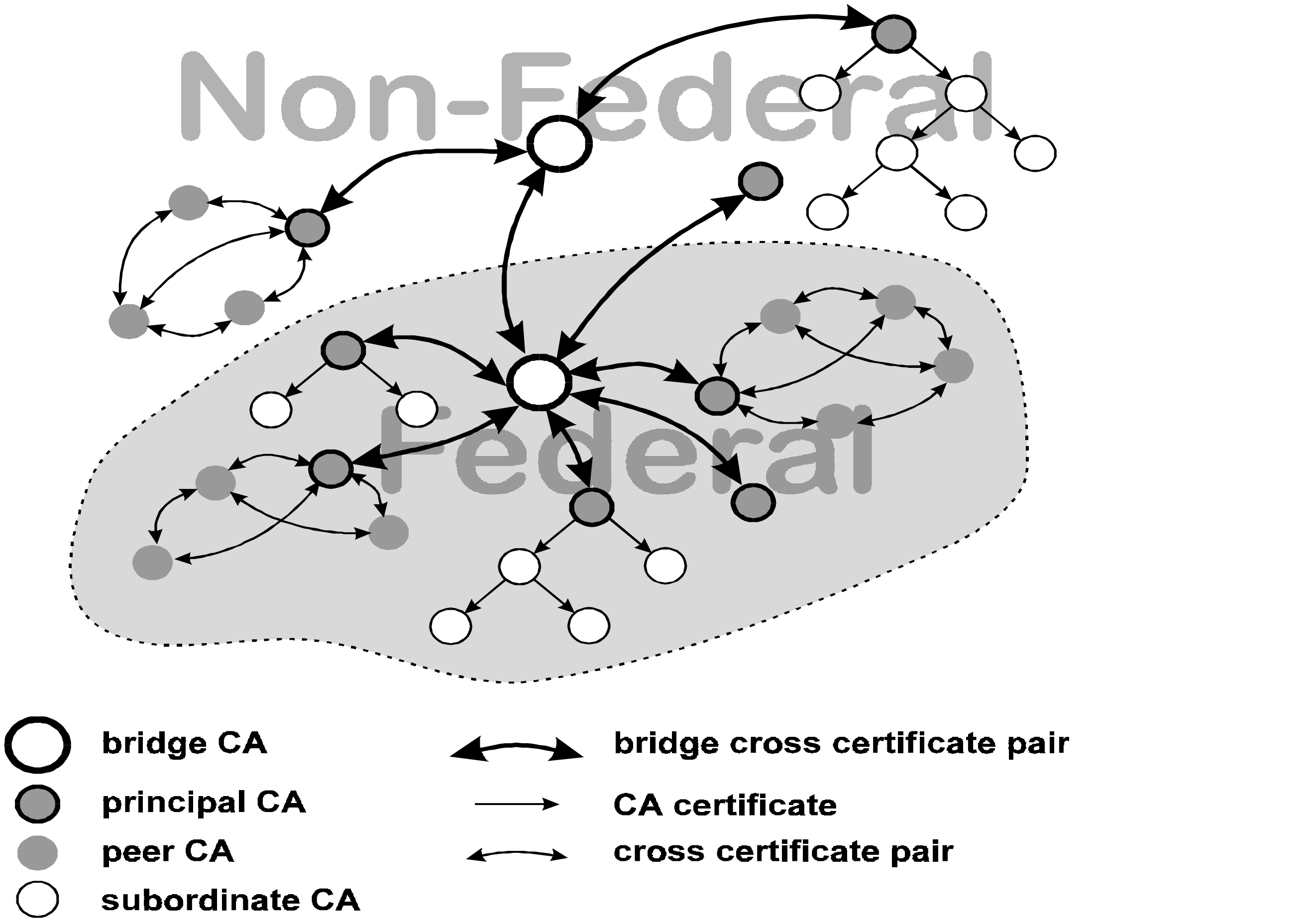
Dave Fillingham, X32
dwfilli@missi.ncsc.mil

3 December 1998

Overview

- Problem overview
- Architecture design considerations
- Proposed directory architecture
- Features of the proposal
- Request for frank appraisal

The Bridge Certification Authority (BCA)



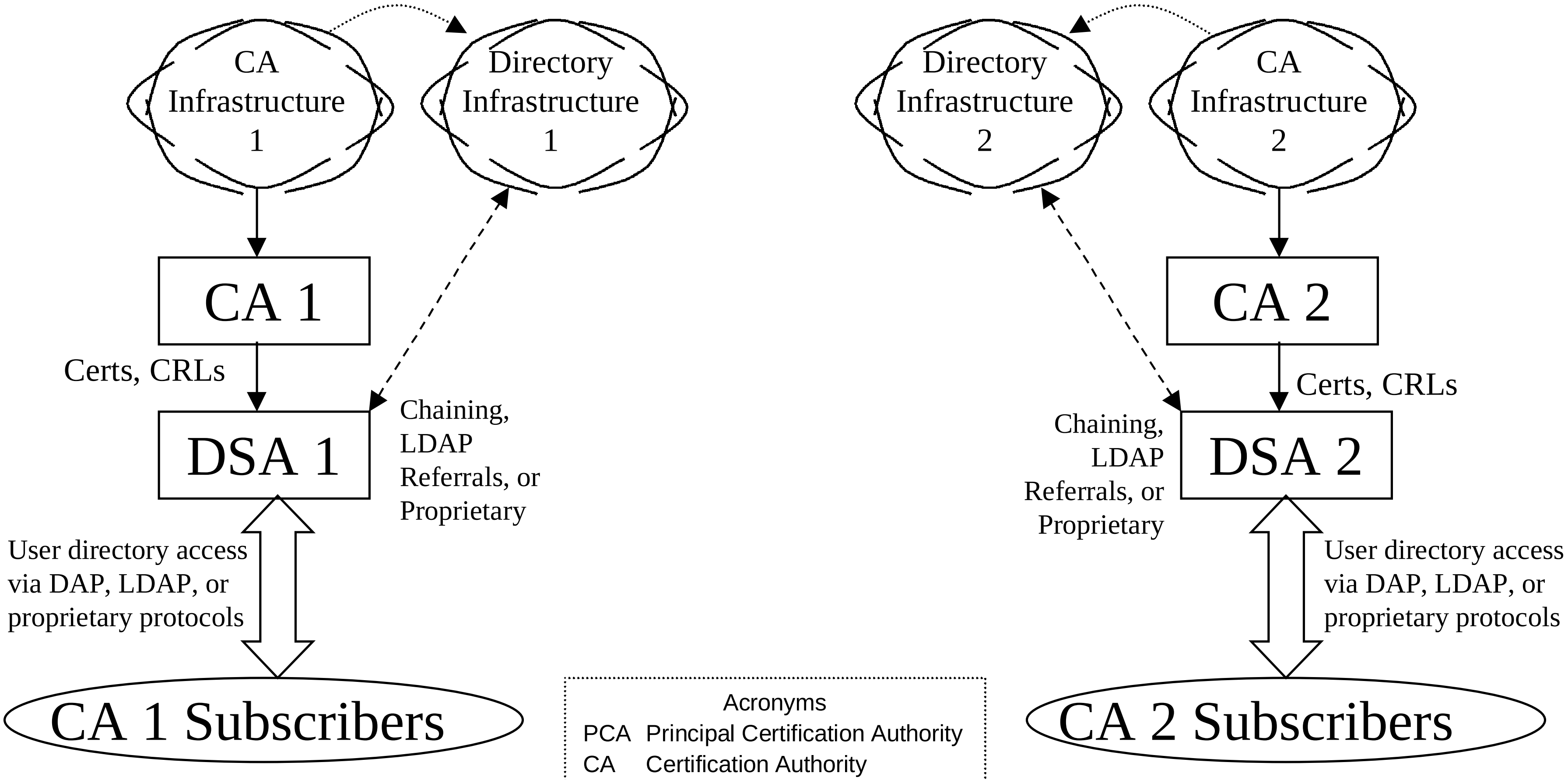
BCA and Directories

- BCA provides trust paths to diverse infrastructures
- BCA concept mostly silent about providing directory/repository services
- Existence of trust paths not enough - applications must be able to retrieve the necessary certificates and (if used) revocation lists

Directory Architecture Considerations

- Design to be specifically oriented toward making the BCA concept work
- Minimize “Federal Requirements”
- Allow for restricting “outside” access to “internal” directories
- Do not impact the clients
- Allow for a “bottom up” implementation

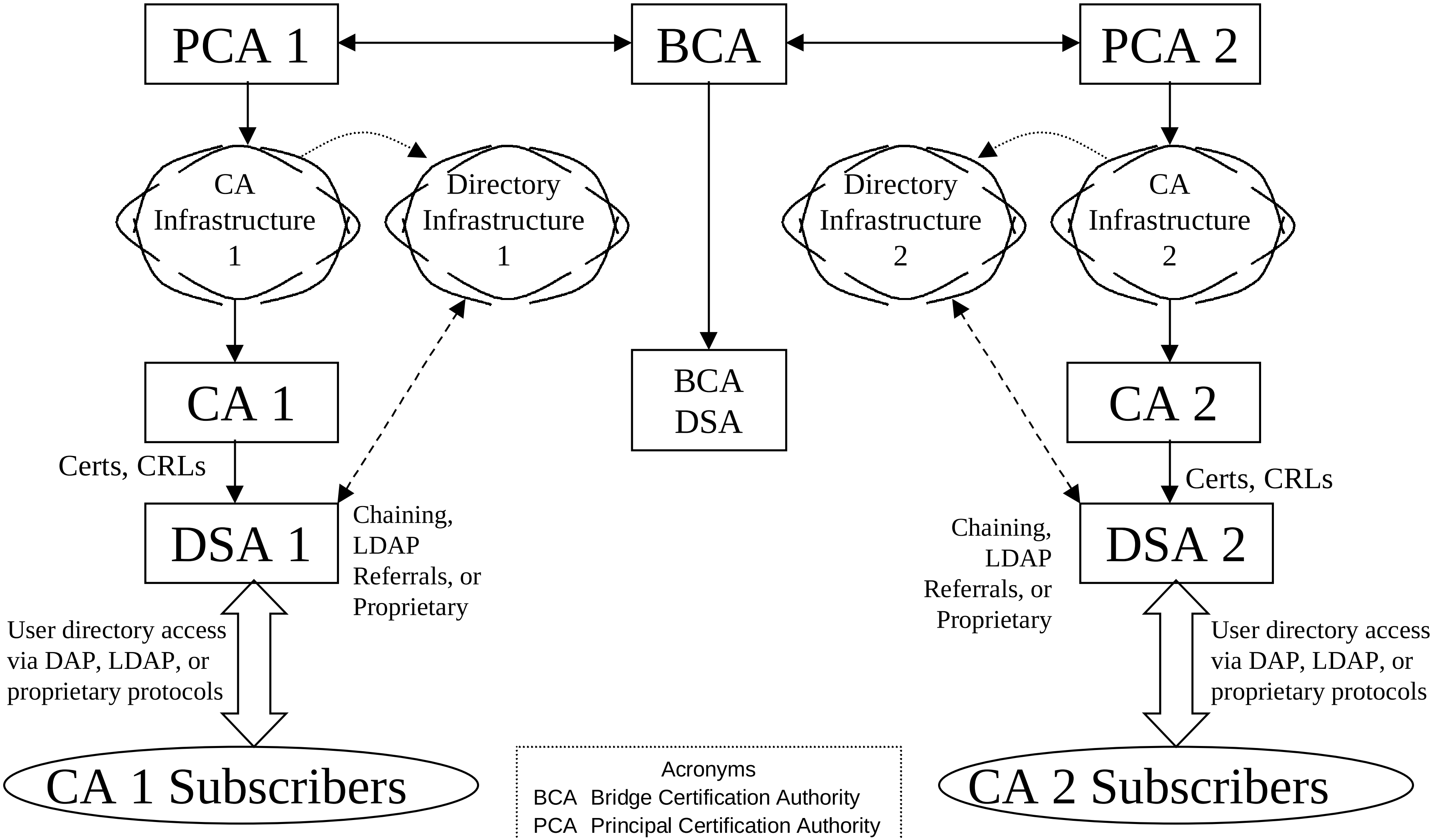
Today’s Stovepipe Public Key Infrastructures


CA Infrastructure 1
Directory Infrastructure 1
Directory Infrastructure 2
CA Infrastructure 2
CA 1
CA 2
Certs, CRLs
Certs, CRLs
DSA 1
DSA 2
Chaining, LDAP Referrals, or Proprietary
Chaining, LDAP Referrals, or Proprietary
User directory access via DAP, LDAP, or proprietary protocols
User directory access via DAP, LDAP, or proprietary protocols
CA 1 Subscribers
CA 2 Subscribers

Acronyms

PCA	Principal Certification Authority
CA	Certification Authority
DSA	Directory System Agent

The BCA Creates Certificate Chains



PCA 1

BCA

PCA 2

CA Infrastructure 1

Directory Infrastructure 1

Directory Infrastructure 2

CA Infrastructure 2

CA 1

BCA DSA

CA 2

Certs, CRLs

Certs, CRLs

DSA 1

Chaining, LDAP Referrals, or Proprietary

Chaining, LDAP Referrals, or Proprietary

DSA 2

User directory access via DAP, LDAP, or proprietary protocols

User directory access via DAP, LDAP, or proprietary protocols

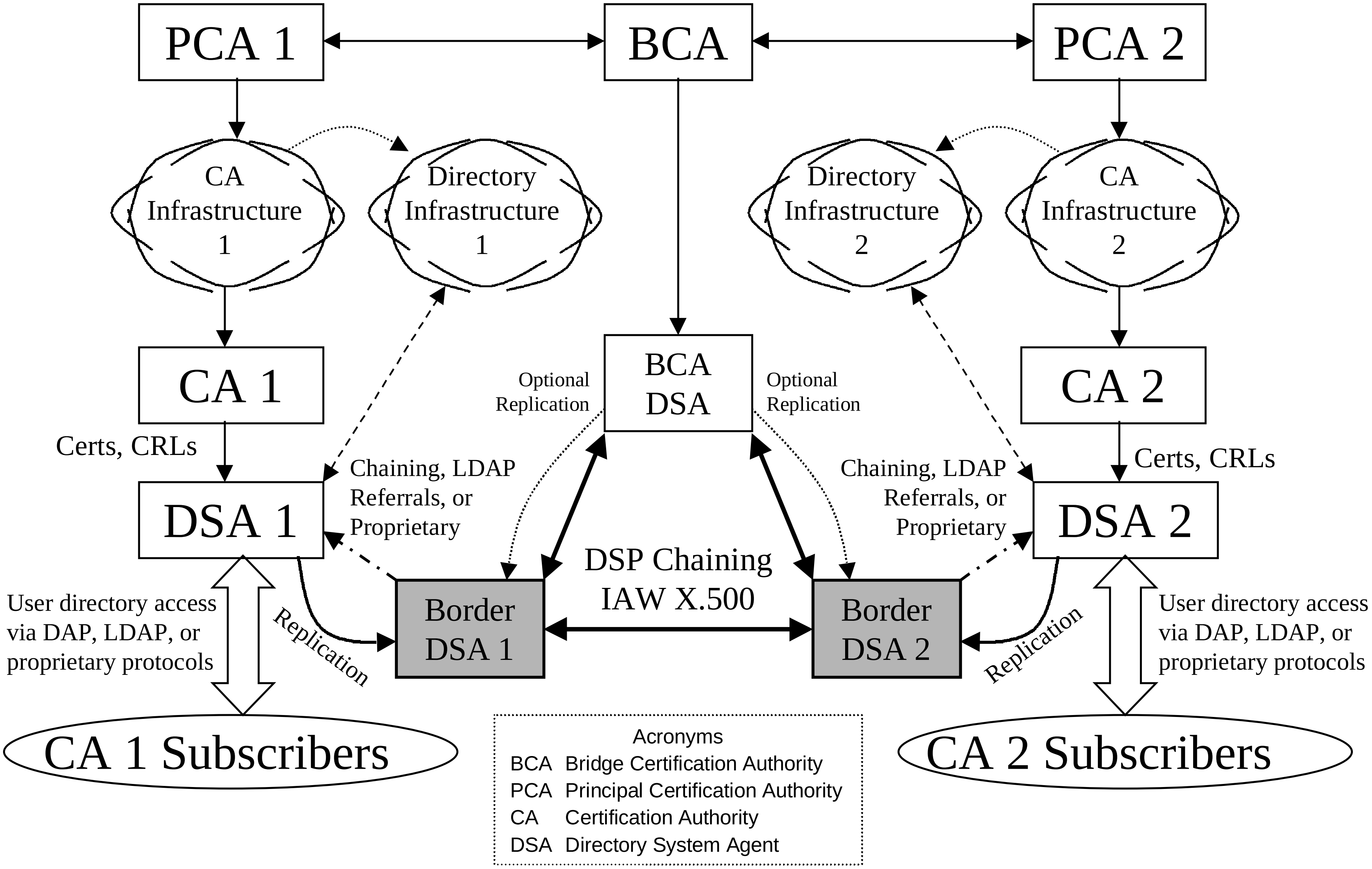
CA 1 Subscribers

CA 2 Subscribers

Acronyms

BCA	Bridge Certification Authority
PCA	Principal Certification Authority
CA	Certification Authority
DSA	Directory System Agent

Chained Border Directories Link the Infrastructures



PCA 1

BCA

PCA 2

CA Infrastructure 1

Directory Infrastructure 1

Directory Infrastructure 2

CA Infrastructure 2

CA 1

BCA DSA

CA 2

Optional Replication

Optional Replication

Certs, CRLs

Certs, CRLs

Chaining, LDAP Referrals, or Proprietary

Chaining, LDAP Referrals, or Proprietary

DSA 1

DSA 2

DSP Chaining IAW X.500

User directory access via DAP, LDAP, or proprietary protocols

User directory access via DAP, LDAP, or proprietary protocols

Replication

Replication

Border DSA 1

Border DSA 2

CA 1 Subscribers

CA 2 Subscribers

Acronyms

BCA	Bridge Certification Authority
PCA	Principal Certification Authority
CA	Certification Authority
DSA	Directory System Agent

Features of the Proposed Approach

- Does not require changes to legacy applications
- Does not impose requirements on client access protocols
- Does not impact CA to Directory/Repository protocols or interactions
- “Border Directory System Agent” concept allow various agencies to implement local policies regarding who accesses which directory entries

Suggested Course of Action

- Federal Public Key Infrastructure Technical Working Group to more thoroughly analyze concept
- Define component functional requirements
- Define required standards
  - Keep the standards simple and minimal!
  - Maximize use of already defined and commercially vetted standards, like the Lightweight Directory Access Protocol (LDAP) Version 2 schema
- Implement a directory demonstration in conjunction with the Bridge Certification Authority demonstration